PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-222022
(43)Date of publication of application : 09.08.2002

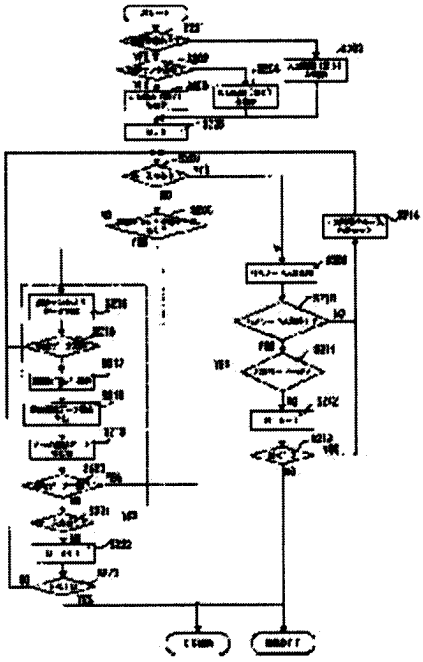
(51)Int.Cl. G06F 1/00
G06F 15/00

(21)Application number : 2001-019476
(22)Date of filing : 29.01.2001

(71)Applicant : TOSHIBA CORP
(72)Inventor : TAMURA SATOSHI

(54) ELECTRONIC EQUIPMENT SYSTEM AND ACTUATING METHOD FOR ELECTRONIC EQUIPMENT SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an actuating method for electronic equipment whose OS starts when either of a password and biological data match registered data as a method for user authentication before OS actuation.
SOLUTION: When the power source of the system is turned on, a control part 3 decides whether fingerprint data are registered in a user identification data storage part 6 and whether a fingerprint sensor 2 is usable and displays a screen urging the input of a password at a display part 6 when a fingerprint is not registered or when the fingerprint sensor 2 is not usable. When fingerprint data are already registered and the fingerprint sensor 2 is usable, a screen urging the input of fingerprint data or a password is displayed at the display part 6. The inputted data are compared with the registered data and it is determined whether the system is actuated according to the comparison result, thus performing OS actuation/shutdown processing.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－222022
（P2002－222022A）
(43)公開日　平成14年８月９日(2002.8.9)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード*(参考)
Ｇ０６Ｆ　1/00	３７０	Ｇ０６Ｆ　1/00	３７０Ｅ	５Ｂ０８５
15/00	３３０	15/00	３３０Ｆ	

審査請求　未請求　請求項の数13　ＯＬ　（全 13 頁）

(21)出願番号　特願2001－19476(P2001－19476)

(22)出願日　平成13年１月29日(2001.1.29)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　田村　聡
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内
(74)代理人　100083161
弁理士　外川　英明

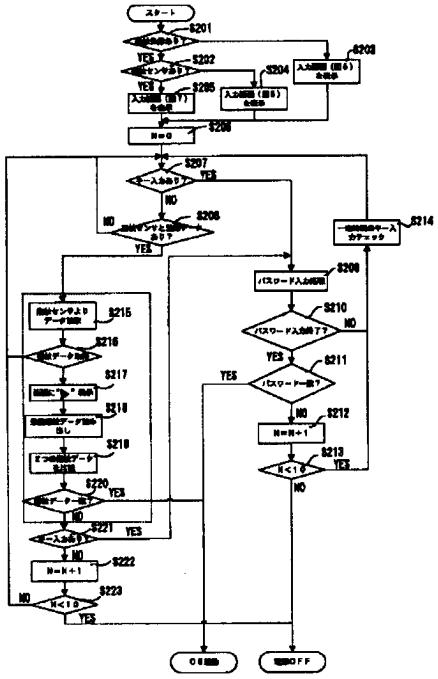
Ｆターム(参考)　5B085 AE03 AE26

(54)【発明の名称】　電子機器システム及び電子機器システムの起動方法

(57)【要約】

【課題】ＯＳ起動前のユーザ認証方法として、パスワードか生体データのどちらか一方が登録しておいたデータと一致すればＯＳが起動する電子機器の起動方法を提供することを目的とする。

【解決手段】システムの電源がＯＮされると、制御部３は、ユーザ識別データ保存部６に指紋データが登録されているか否か、また、指紋センサ２が使用可能であるか否かを判断し、予め指紋が登録されていない、又は指紋センサ２が使用可能状態に無い場合は、表示部６にパスワードの入力を促す画面を表示する。予め指紋データ登録済みで且つ指紋センサ２が使用可能状態であれば、指紋データ若しくはパスワードのどちらかの入力を促す画面を表示部６に表示する。入力されたデータと登録済みのデータとを照合し、照合結果に応じてシステムの起動可否を決定し、ＯＳ起動／シャットダウンの処理を行う。



【特許請求の範囲】

【請求項１】使用者の本人確認を行う電子機器システムであって、前記使用者の生体データを入力する手段と、パスワードを入力する文字入力手段と、前記使用者の生体データ及びパスワードを予め記憶する記憶手段と、前記電子機器システムへの電源投入時に、生体データ又はパスワードを入力する旨の指示を提示する指示手段と、前記生体データ入力手段から生体データを入力された場合は、前記記憶手段に記憶されている生体データとの照合を行ない、前記文字入力手段からパスワードの入力があった場合は、前記記憶手段に予め記憶されているパスワードとの照合を行なう照合手段と、前記照合手段の照合結果に応じて、前記電子機器システムの使用可否を制御する制御手段とを具備することを特徴とする電子機器システム。

【請求項２】前記生体データは、使用者の指紋データであることを特徴とする請求項１に記載の電子機器システム。

【請求項３】前記生体データ入力手段はPCカードであり、前記電子機器システムに着脱可能に接続することを特徴とする請求項１に記載の電子機器システム。

【請求項４】前記制御手段はさらに、前記記憶手段に予め生体データが記憶されているか否かを判断し、前記記憶手段に予め生体データが記憶されていないと判断した場合、前記指示手段へパスワードの入力のみを促すことを指示し、前記指示手段は、パスワードの入力のみを促すことを特徴とする請求項１記載の電子機器システム。

【請求項５】前記記憶手段に記憶されている前記パスワードを削除する場合、前記記憶手段に記憶している生体データも削除することを特徴とする請求項１に記載の電子機器システム。

【請求項６】電子機器本体と、前記電子機器本体に着脱可能に接続する生体データ入力部とからなり、使用者の本人確認を行う電子機器システムであって、前記生体データ入力部は、前記使用者の生体データを入力する手段と、前記生体データを用いて、使用者の確認を実行するプログラムを記憶する第１の記憶手段とを具備し、前記電子機器本体は、パスワードを入力する文字入力手段と、前記使用者の生体データ及びパスワードを予め記憶している第２の記憶手段と、使用者に、生体データまたはパスワードの入力の操作を促す指示手段とを具備し、前記電子機器本体はさらに、前記第１の記憶手段から前記プログラムを読み込み、前記指示手段により生体データまたはパスワードの入力を促し、前記生体データ入力部から生体データの入力が行なわれた場合は、前記第２の記憶手段に記憶されている生体データとの照合を行ない、前記文字入力手段からパスワードの入力があった場合は、前記パスワードとの照合を行なう照合手段と、前記照合手段の照合結果に応じて、前記電子機器本体の使用可否を制御する制御手段とを具備することを特徴とする電子機器システム。

【請求項７】前記生体データは、使用者の指紋データであることを特徴とする請求項６に記載の電子機器システム。

【請求項８】前記生体データ入力部は、ＰＣカードであり、前記電子機器本体が具備するＰＣカードスロットルに着脱可能に接続することを特徴とする請求項６に記載の電子機器システム。

【請求項９】前記第２の記憶手段に記憶している前記パスワードを削除する場合、前記第２の記憶手段に記憶している生体データも削除することを特徴とする請求項６に記載の電子機器システム。

【請求項１０】前記生体データ入力部が前記電子機器本体に接続していない場合、若しくは前記第２の記憶手段に予め生体データが記憶されていない場合、前記指示手段は、パスワードの入力指示のみを促す指示を出すことを特徴とする請求項６記載の電子機器システム。

【請求項１１】生体データを入力する手段と、パスワードを入力する手段とを具備する電子機器システムの起動方法であって、使用者に、生体データまたはパスワードの入力を促し、前記生体データ入力手段から生体データを入力された場合は、前記電子機器システムが具備する第１の記憶手段に登録している生体データとの照合を行ない、前記文字入力手段からパスワードの入力があった場合は、前記第１の記憶手段に記憶されているパスワードとの照合を行ない、照合結果に応じて、前記電子機器システムの使用可否を制御することを特徴とする電子機器システムの起動方法。

【請求項１２】前記生体データは指紋データを用いることを特徴とする請求項１１記載の電子機器システムの起動方法。

【請求項１３】生体データを入力する生体データ入力手段と、パスワードを入力する文字入力手段とを具備する電子機器システムの起動方法であって、前記電子機器システムの電源が投入された際に、予め使用者の生体データが登録されているか否か判断し、前記生体データ入力手段が使用可能であるか否か判断し、予め生体データの登録が成されており且つ前記生体データ入力手段が使用可能状態である場合は、生体データ、若しくはパスワードの入力を促し、前記生体データ入力手段から生体データを入力された場合は、予め登録されている生体データとの照合を行ない、前記文字入力手段からパスワードの入力があった場合は、予め登録されているパスワードとの照合を行ない、照合結果に応じて、電子機器システムの使用可否を制御し、前記生体データが登録されていない場合、若しくは前記生体データ入力手段が使用不可能状態である場合は、パスワードの入力を促し、前記文字入力手段から入力されるパスワードと、予め登録されているパスワードとの照合を行い、照合結果に応じて、電子機器システムの使用可否を制御することを特徴とする

電子機器システムの起動方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、生体データを用いる電子機器システムおよび電子機器システムの起動方法に関する。

【０００２】

【従来の技術】従来、パーソナルコンピュータ（以後、パソコンと称す）等の電子機器を起動する際に、特定ユーザを認証する方法として、文字・数字の組合せから成るパスワードを照合して、ユーザを認証する方法（以後、パスワード認証方法と称す）が用いられている。

【０００３】また、近年、パスワード認証方法以外にも、指紋に代表される生体データを照合してユーザを認証する方法（以後、指紋認証方法と称す）も急速に普及して来ている。

【０００４】特に、指紋認証方法は、１．パスワード方法に比べてキーボードを使った入力を必要としない、２．パスワードのように覚えておく必要がない、３．指紋情報は他人と異なるなど、簡便さ及びセキュリティ面で有効的な方法である。

【０００５】このような指紋認証による電子機器のセキュリティとしては、特開２０００－１２２９７５公報では、指紋を含む複数のバイオメトリクスデータをユーザ確認手段として用い、ログオン許可などを実現するバイオメトリクスによるユーザ確認システム及び記憶媒体が開示されている。

【０００６】また、特登　２９６７７６４号公報では、非接触ICカードにより指紋認証を行った結果をコンピュータに送信しログインをすると言った、非接触ＩＣカードおよびそれを用いたログイン方法といった技術が開示されている。

【０００７】

【発明が解決しようとする課題】しかし、上記従来技術では、特開２０００－１２２９７５公報では、確認手段の一つに、生体データを用いるが、使用者側で、ログイン時の照合方式を自由に選択することが可能となっているが、選択した認証方法全てについて、照合をする必要があり、全ての照合について、許可になった場合のみ電子機器のログオン許可となるため、その選択した照合方式が一つでも、マッチし無かった場合にログオンはできない。また、その照合に要する生体データが複数あるため、どの生体データを登録しているのか等データ管理が困難である。

【０００８】また、特登　２９６７７６４号公報記載の非接触カードを用いる場合では、必ず、カードとシステムとが同じ無線方式に応じたものでことが必要となる。また、カード側に、指紋登録データ及び、パスワードとを記憶しているので、カードを紛失した場合などに、システムにログインすることができなくなるといった問題がある。

【０００９】さらに、ログイン方法が、生体データのみによるものである場合は、例えば指紋のみの認証では指紋に傷がついたときなど、指紋の情報に変化が起こった場合に、ユーザ本人であるのに認証で拒否されてしまい、その後システムへのログインを拒否されることが考えられる。

【００１０】そこで、本発明では電子機器システム起動時のユーザ認証方法として、セキュリティ面で有用で且つ、指紋情報に変化が起こった場合でも柔軟に対応可能な電子機器システムおよび電子機器システムの起動方法を提供することを目的とする。

【００１１】

【課題を解決するための手段】上記目的を達成する為に、請求項１にかかる発明では、使用者の本人確認を行う電子機器システムであって、使用者の生体データを入力する手段と、パスワードを入力する文字入力手段と、使用者の生体データ及びパスワードを予め記憶する記憶手段と、電子機器システムへの電源投入時に、生体データ又はパスワードを入力する旨の指示を提示する指示手段と、生体データ入力手段から生体データを入力された場合は、記憶手段に記憶されている生体データとの照合を行ない、文字入力手段からパスワードの入力があった場合は、記憶手段に予め記憶されているパスワードとの照合を行なう照合手段と、照合手段の照合結果に応じて、電子機器システムの使用可否を制御する制御手段とを具備することを特徴とする。

【００１２】このような構成により、電子機器起動時の使用者認証において、生体データもしくはパスワードの入力により電子機器の起動可否を制御可能であり、生体データに変化が起き、生体データによる使用者認証ができなくなった場合でも、パスワードによる使用者認証が可能であり、使用者認証が柔軟に対応可能である電子機器システムを提供することが可能となる。

【００１３】また、請求項６にかかる発明では、電子機器本体と、電子機器本体に着脱可能に接続する生体データ入力部とからなり、使用者の本人確認を行う電子機器システムであって、生体データ入力部は、使用者の生体データを入力する手段と、生体データを用いて、使用者の確認を実行するプログラムを記憶する第１の記憶手段とを具備し、電子機器本体は、パスワードを入力する文字入力手段と、使用者の生体データ及びパスワードを予め記憶している第２の記憶手段と、使用者に、生体データまたはパスワードの入力の操作を促す指示手段とを具備し、電子機器本体はさらに、第１の記憶手段からプログラムを読み込み、指示手段により生体データまたはパスワードの入力を促し、生体データ入力部から生体データの入力が行なわれた場合は、第２の記憶手段に記憶されている生体データとの照合を行ない、文字入力手段からパスワードの入力があった場合は、パスワードとの照

合を行なう照合手段と、照合手段の照合結果に応じて、電子機器本体の使用可否を制御する制御手段とを具備することを特徴とする。

【００１４】このような構成により、電子機器起動時の使用者認証において、生体データによる認証が可能か否か判断し、生体データ認証が可能な場合は、生体データ若しくはパスワードの入力により電子機器の起動可否を制御可能であり、生体データ認証ができない場合は、パスワードの認証を使用者に促し、状況に応じて、認証処理を柔軟に対応可能とする電子機器システムを提供することが可能となる。

【００１５】また、請求項１１にかかる発明では、生体データを入力する手段と、パスワードを入力する手段とを具備する電子機器システムの起動方法であって、使用者に、生体データまたはパスワードの入力を促し、生体データ入力手段から生体データを入力された場合は、電子機器システムが具備する第１の記憶手段に登録している生体データとの照合を行ない、文字入力手段からパスワードの入力があった場合は、第１の記憶手段に記憶されているパスワードとの照合を行ない、照合結果に応じて、電子機器システムの使用可否を制御することを特徴とする。

【００１６】このような構成により、電子機器起動時の使用者認証において、生体データもしくはパスワードの入力により電子機器の起動可否を制御可能であり、生体データに変化が起き、生体データによる使用者認証ができなくなった場合でも、パスワードによる使用者認証が可能であり、使用者認証が柔軟に対応可能である電子機器システムの起動方法を提供することが可能である。

【００１７】また、請求項１３にかかる発明では、生体データを入力する生体データ入力手段と、パスワードを入力する文字入力手段とを具備する電子機器システムの起動方法であって、電子機器システムの電源が投入された際に、予め使用者の生体データが登録されているか否か判断し、生体データ入力手段が使用可能であるか否か判断し、予め生体データの登録が成されており且つ生体データ入力手段が使用可能状態である場合は、生体データ、若しくはパスワードの入力を促し、生体データ入力手段から生体データを入力された場合は、予め登録されている生体データとの照合を行ない、文字入力手段からパスワードの入力があった場合は、予め登録されているパスワードとの照合を行ない、照合結果に応じて、電子機器システムの使用可否を制御し、生体データが登録されていない場合、若しくは生体データ入力手段が使用不可能状態である場合は、パスワードの入力を促し、文字入力手段から入力されるパスワードと、予め登録されているパスワードとの照合を行い、照合結果に応じて、電子機器システムの使用可否を制御することを特徴とする。

【００１８】このような構成により、電子機器起動時の使用者認証において、生体データによる認証が可能か否か判断し、生体データ認証が可能な場合は、生体データ若しくはパスワードの入力により電子機器の起動可否を制御可能であり、生体データ認証ができない場合は、パスワードの認証を使用者に促し、状況に応じて、認証処理を柔軟に対応可能とする電子機器システムの起動方法を提供することが可能である。

【００１９】

【発明の実施の形態】以下本発明に係る実施の形態を、図面を参照して説明する。

【００２０】本実施形態では、生体データとして、指紋データを用いる例について説明する。

【００２１】図１に、本実施形態に係る、電子機器システムのハードウェア構成図を示す。

【００２２】ユーザインターフェースとして、キーボード１と指紋センサ２を具備し、これらは、システム全体の制御および、ログイン認証処理の制御を司る制御部３に接続している。

【００２３】この制御部３には、ログイン認証処理の認証プログラムを保存する認証プログラム保存部４と、ユーザが登録したパスワードおよび指紋データを保存するユーザ識別データ保存部５とが接続している。

【００２４】また、ユーザに対し、各種情報や操作を促すための情報を提示するための表示部６も、制御部３と接続している。

【００２５】キーボード１は、本システムのユーザインターフェースの１つであり、通常は、システムの操作を行なうが、文字・数字の組合せから成るパスワードを入力する際にも用いる。

【００２６】指紋センサ２は、指紋データを入力する際のインターフェースであり、表示部６に表示される指示に従い、指紋センサ２に指を接触させることにより、ユーザの指紋を読み込むものである。この指紋センサ２は、このシステムに内蔵されるものも考えられるが、その他に、ＰＣカードのものや、ＵＳＢにより接続するものなどが考えられる。

【００２７】制御部３は、システム全体の制御を司り、認証プログラム保存部４から、指紋認証プログラムを読出し、認証プログラムを実行、制御するものである。

【００２８】認証プログラム保存部４は、後述する指紋認証プログラムを記憶しており、制御部３により読み出される。

【００２９】ユーザ識別データ保存部５は、ユーザが登録した文字・数字から成るパスワード及びユーザの指紋データを記憶保存するものであり、ユーザ毎にパスワードと指紋データとを記憶している。

【００３０】表示部６は、ユーザに対して視覚的に情報を提示するものであり、ＣＲＴやＬＣＤなどの表示装置が用いられる。

【００３１】図２に、電子機器システムの例の斜視図を

示す。

【００３２】本発明に係る電子機器システムの例として、図２のようなパソコン１３が挙げられる。

【００３３】パソコン１３は、本体ケース１２と表示部ケース１３と表示部６とキーボード１とを有する。本体ケース１２はその上面部にキーボード１を配設している。本体ケース１２と表示部ケース１３とは、ヒンジ部１４により回動可能に接続している。表示部ケース１３は、表示部６の表示領域が可視状態となるよう表示部６の周辺部を保持している。本体ケース１２側面にはＰＣカードを着脱可能に接続するＰＣカードスロット１５を有し、このＰＣカードスロット１５に、ＰＣカードの形で提供される指紋センサ２が挿入している。

【００３４】次に、まずユーザ認証の核となる指紋認証の処理について図３を用いて説明する。図３は、指紋認証プログラムのフローチャートである。

【００３５】まず、制御部３が認証プログラム保存部４から、指紋認証プログラムを読み出し（ステップＳ１０１）、以後説明する認証プログラムを実行する。

【００３６】指紋認証プログラムでは、まず指紋センサ２からユーザの指紋データを読取る(ステップＳ１０２)。ここで、指紋センサ２により指紋データが読取れなければ（ステップＳ１０２のＮＯ）、エラー処理１を行なう（ステップＳ１０３）。

【００３７】エラー処理１は、表示部６に、指紋データが読み取れない旨のメッセージの表示を行なったり、図示しないスピーカから警告音を発生させるなど、ユーザに読取エラーであることを通知する。

【００３８】指紋センサ２により指紋データが読取れた場合（ステップＳ１０２のＹＥＳ）、次のステップで既に登録されている指紋データ（以後、既登録データと称す）との比較を行なう。

【００３９】指紋データが読み取れた際に、制御部３がユーザ識別データ保存部５から、既登録データを読み出す（ステップＳ１０４）。指紋センサ２により読みとった指紋データ（以後、認証対象データ）と、既登録データとを比較し（ステップＳ１０５）、２つのデータが一致していた場合には（ステップＳ１０５のＹＥＳ）、ユーザ認証成功となり指紋認証処理を終了する。

【００４０】ここで、ユーザ識別データ保存部６に複数の指紋データが登録されている場合には、これら複数の既登録データと認証対象データとの比較を繰り返す。

【００４１】既登録データと認証対象データとが一致しない場合（ステップＳ１０６のＮＯ）、エラー処理２を行なう（ステップＳ１０７）。エラー処理２では、表示部６に指紋センサ２により読みとった指紋データが、既登録データと一致しない旨のメッセージを表示させる。また、さらに他の指を指紋センサにより読み取るように促すメッセージを表示しても良い。

【００４２】上記のように、ユーザの指紋認証処理が行なわれる

【００４３】続いて、上述した指紋認証プログラムを利用して、パスワードまたは指紋によるユーザ認証処理を行なうフローチャートを図４に示す。

【００４４】まずシステムの電源がＯＮされると、制御部３は、ユーザ識別データ保存部６に指紋データが登録されているか否かをチェックする（ステップＳ２０１）。

【００４５】なんらかの指紋データが登録されていると（ステップＳ２０１のＹＥＳ）、次に指紋センサ２の有無を確認する（ステップＳ２０２）。これは、指紋センサ２がＰＣカードの形状をしたものや、ＵＳＢにより接続するものである場合や、別途電源供給を受けている場合などが考えられるためであり、指紋センサ２が使用可能であるか否かを判断する。

【００４６】上記ステップＳ２０１とステップＳ２０２の判定により表示部６に表示する入力画面を３種類に分ける。

【００４７】指紋が登録されていない場合（ステップＳ２０１のＮＯ）は、図５に示す入力画面を表示部６に表示し（ステップＳ２０３）、指紋データは登録されているが（ステップＳ２０１のＹＥＳ）、指紋センサ２が無い（電源ＯＦＦ、非接続等）場合（ステップＳ２０２のＮＯ）は、図６に示す入力画面を表示部６に表示する（ステップＳ２０４）。指紋データが登録されており（ステップＳ２０１のＹＥＳ）、且つ指紋センサ２がある（電源ＯＮ、接続済み等）場合（ステップＳ２０２のＹＥＳ）は図７に示す入力画面を表示部６に表示する（ステップＳ２０５）。

【００４８】図５乃至図７に示す入力画面は、ユーザに対して、ユーザがどのような認証処理を行えば良いのかを明確にするためである。

【００４９】夫々、入力画面表示後、ユーザ認証エラーの際に、リトライの機会を与える為のエラーカウント変数“Ｎ”を０にセットする（ステップＳ２０６）。

【００５０】まず、指紋センサ若しくは登録された指紋データ（既登録データ）が無い場合について説明する。

【００５１】指紋センサ２及び既登録データが無い場合は、指紋認証を行うことができ無いため、パスワードによるログイン処理のみを行なう。よってステップＳ２０７のキー入力の判定を行ないキー入力が無い場合（ステップＳ２０７のＮＯ）は、指紋センサ２若しくは登録指紋データも無いので（ステップＳ２０８のＮＯ）、再びステップＳ２０７に戻り、キー入力が行なわれるまで、このループを繰り返す。

【００５２】キー入力が有ると（ステップＳ２０７のＹＥＳ）、パスワードによる認証処理を開始する。

【００５３】パスワード認証処理（ステップＳ２０９）では、キーボード１から入力された数字・文字を保存し、パスワード入力終了する（リターンキーが押され

る）までに入力された文字列をユーザから入力されたパスワードとして判断する。

【００５４】パスワード入力終了の判定（ステップＳ２１０）でパスワード入力が終了された場合（ステップＳ２１０のＹＥＳ）、入力されたパスワードとユーザ識別データ保存部５に保存されているパスワード（予めユーザが登録しておいたパスワード）との比較をおこなう（ステップＳ２１１）。

【００５５】パスワード入力が終了していない場合は（ステップＳ２１０のＮＯ）、次のキー入力を待つ為に一定時間のキー入力チェックを行なう（ステップＳ２１４）。キー入力があれば（ステップＳ２０７のＹＥＳ）、再びキーボード１から入力された数字・文字を保存し、パスワード入力終了か否かのチェックを行なう（ステップＳ２１０）。

【００５６】パスワードが一致した場合には、パスワードが一致したことを表示部６に表示し、ＯＳ起動の処理を行なう。パスワードが一致し、認証に成功したときの画面表示例を図８に示す。

【００５７】パスワードが一致しなかった場合（ステップＳ２１１のＮＯ）は、エラーカウント変数“Ｎ”を加算する（ステップＳ２１２）。次に、所定のエラー許可回数と“Ｎ”との値を比較する（ステップＳ２１３）。本例では、エラー許可回数を１０とする。エラー許可回数を越えていない場合（ステップＳ２１３のＹＥＳ）、一定時間のキー入力待ち（ステップＳ２１４）状態から、ステップＳ２０７のキー入力処理に戻り、上述したパスワード入力処理を改めて開始する。この際、前回入力されたパスワードをクリアする。

【００５８】エラー許可回数を越えていた場合（ステップＳ２１１のＹＥＳ）は電源をＯＦＦする。

【００５９】エラー許可回数は、ユーザに入力ミスの猶予を与えるための数値である。ユーザの入力ミスをカウントし、予め決められたエラー許可回数（本例では１０回）を越えるまでは、再び認証のための入力処理をおこなうが、エラー許可回数を越えた場合には、ＯＳを使うことのできるユーザではないと判断する。本件ではこの場合の処理として電源OFFをおこなう。

【００６０】次に、指紋が登録されていて、且つ指紋センサ２を具備する場合のパスワード認証処理と指紋認証処理について説明する。

【００６１】まず、キー入力が有るか否かの判断を行い（ステップＳ２０７）、キー入力があれば（ステップＳ２０７のＹＥＳ）、前述したパスワード認証処理を行なう。

【００６２】キー入力が無い場合（ステップＳ２０７のＮＯ）は、次に、指紋センサ２と登録指紋データがあるか否かを判断する（ステップＳ２０８）。

【００６３】ここでは、指紋センサ２も登録指紋データもある場合を想定しているので（ステップＳ２０８のＹＥＳ）、指紋認証処理へ進む。図９に指紋認証の画面表示初期状態の図を示す。

【００６４】指紋認証処理（点線で囲まれた部分、ステップＳ２１５乃至ステップＳ２２０）は、途中、画面表示を行う処理（ステップＳ２１７）を除いて図３で説明したものと同じである。

【００６５】指紋認証処理が開始されると、制御部３は、認証プログラム保存部４から指紋認証プログラムを読取る。

【００６６】まず、指紋センサ２から指紋データを読み取る（ステップＳ２１５）。指紋データの読取りに成功すると（ステップＳ２１６のＹＥＳ）、図１０に示す画面表示例のように指紋データが読み取れたことを表示部６を介して通知する。指紋データの読取りができなければ（ステップＳ２１６のＮＯ）、指紋認証処理を終了し、ステップＳ２０７へ戻る。

【００６７】指紋データが読み取れた場合（ステップＳ２１６のＹＥＳ）、次に読みとった指紋データと、ユーザ識別データ保存部５に記憶している既登録データとの比較を行なう（ステップＳ２１９）。指紋データが一致すれば（ステップＳ２２０のＹＥＳ）、指紋データが一致したことを表示部６に表示し、ＯＳ起動の処理をおこなう。認証に成功した場合の画面表示例は図８に示したものと同じである。指紋データが一致しない場合には（ステップＳ２２０のＮＯ）、キー入力があるか否かの判定を行ない（ステップＳ２２１）、キー入力があれば（ステップＳ２２１のＹＥＳ）パスワード認証処理へ移行する。指紋認証に失敗した場合の画面表示例を図１１に示す。

【００６８】キー入力が無い場合は（ステップＳ２２１のＮＯ）、エラーカウント変数“Ｎ”を加算する（ステップＳ２２２）。次に、所定のエラー許可回数と“Ｎ”との値を比較する（ステップＳ２２３）。

【００６９】“Ｎ”がエラー許可回数以内である場合は、再びステップＳ２０７へ戻り、キー入力判定を行なう。

【００７０】上記した一連の処理をエラー許可回数（本例では１０回）だけ繰り返す。１０回連続して指紋認証処理を行なった場合の画面表示例を図１２に示す。

【００７１】これは１０回連続で指紋データを読取ることはできたが、既登録指紋データとは一致しなかったことを示している。また、本件ではエラー許可回数を１０回としているが、これは何回でもよく、ユーザにより設定することも可能である。

【００７２】１０回の指紋認証処理を行ってもユーザ認証ができない場合は（ステップＳ２２３のＹＥＳ）、ＯＳを使うことのできるユーザではないと判断する。本件ではこの場合の処理として電源OFFをおこなう。

【００７３】本例ではパスワードと指紋認証とのエラー許可回数を同じ変数“Ｎ”同一にカウントしているが、

別々に変数を設けて、夫々エラー許可回数を設定することも可能である。

【００７４】上記のように、本発明では、パスワード若しくは指紋データによるユーザ認証処理を行うことが可能であり、ユーザに対して、２通りの認証手段を提示し、どちらかの認証に成功すれば、システムの起動を行なうものである。このことによって、パスワードを忘れてしまった場合は指紋認証によるログインが可能であり、指紋が傷付いてしまった場合などには、パスワードによるログインが可能であるため、様々なアクシデントに柔軟に対応可能な電子機器システム及びその起動方法を提供することが可能となる。

【００７５】続いて、サスペンド、休止状態からの復帰の際の認証処理について図１３を用いて説明する。図１３はサスペンド／休止状態から、ＰＣを使用状態へ復帰するの際のフローチャートである。

【００７６】図４を用いて説明した処理は、サスペンド、休止状態からの復帰時にも利用可能である。

【００７７】まず、サスペンド、若しくは休止状態から、復帰する時に、図４を用いて説明した認証処理が行われる（ステップＳ３０１）。

【００７８】パスワード若しくは指紋認証によりユーザが認証された場合は（ステップＳ３０２のＹＥＳ）、ＯＳへ復帰する（ステップＳ３０３）。

【００７９】のような処理を行う。この場合、認証されないときは電源OFFするのではなく、それぞれサスペンド、休止状態に戻す。

【００８０】次に、指紋データをユーザ識別データ保存部６へ登録する場合について説明する。

【００８１】指紋の登録と削除についてはＯＳ上のユーティリティソフトを用いて行う。図１４にユーティリティソフトの画面例を示す。

【００８２】図１４の指紋ユーティリティ画面１１は、パスワードを入力する欄１２と、指紋登録及び、指紋データの更新を行うためのボタン１３と、指紋データを削除する際のボタン１４と、この画面を終了するボタン１５が表示される。

【００８３】パスワード欄１２は、ユーザの登録パスワードを入力するボックスであり、ここで、ユーザのパスワードを入力し、ユーザ確認を行なうと、指紋データの登録／更新および削除を行なうことが可能となる。本指紋登録ユーティリティは、パスワードが登録されていない場合は、指紋登録を行なうことができないようになっている。なお、本例では、このパスワードは、電子機器システム起動時のパスワードと同じものであるが、別に登録するものとしても良い。

【００８４】指紋データ登録／更新ボタン１３は、ユーザ認証が完了した場合に、そのユーザの指紋データを登録することが可能となる。

【００８５】指紋削除ボタン１４は、登録済みの指紋データを削除する場合に用いる。

【００８６】キャンセルボタン１５は、この指紋ユーティリティ画面１１を終了する際に用いるものである。

【００８７】次に、指紋データを登録する際の処理について、図１５に指紋データ登録のフローチャートを示す。

【００８８】まず、指紋データ登録を行なうために指紋ユーティリティソフトを起動する。この際に、ユーザのパスワードがユーザ識別データ保存部５に登録されているか否かのチェックを行い（ステップＳ４０１）、パスワードが登録されていない場合は（ステップＳ４０１のＮＯ）、ダイアログ等でエラーメッセージの表示を行ないユーティリティを起動しない（ステップＳ４０２）。これは、本発明では指紋を登録するためにはそれに対応するユーザのパスワードが必要であるためである。

【００８９】パスワードがユーザ識別データ保存部５に登録されていれば（ステップＳ４０１のＹＥＳ）、図１４に示すユーティリティ画面１１を表示する

【００９０】ここで、ユーティリティにパスワードを入力して、指紋登録／更新ボタン１３を押すと、パスワードの認証が行われる。ここで、パスワードが間違っていれば、パスワードが間違っていることを表示部６を介してユーザに通知する。パスワードが正しく、認証が成功した場合は、指紋登録処理を開始する。

【００９１】指紋登録処理では、指紋センサ２から指紋データの読み取りを行い（ステップＳ４０６）、指紋データを読取れれば（ステップＳ４０７のＹＥＳ）、そのデータをユーザ識別データ保存部５へと保存する（ステップＳ４０８）。指紋データが読取れなかった場合（ステップS４０７のＮＯ）には、再び指紋データの取得を行うか、登録を終了するかを選択することが可能である（ステップS４０９）。ここで、再び指紋データの登録を選択すると（ステップS４０９のＹＥＳ）、ステップS４０６に戻り、指紋センサ２から指紋データの読取を行なう。指紋データの登録を終了する場合（ステップS２０９のＮＯ）は、指紋ユーティリティを終了する。

【００９２】また、ステップＳ４０８において、指紋データの登録を行なうと、他の指紋データの登録も行なうことが可能である。複数の指紋登録が可能である。

【００９３】次に、登録されている指紋データを削除する場合について説明する。

【００９４】指紋データの削除は、図１４に示した指紋ユーティリティを使って行う。方法は指紋ユーティリティを起動しパスワードを入力後、指紋削除ボタン１４を押す。

【００９５】パスワードが一致すれば、登録している指紋データを削除することができる。一人で複数登録している場合は、登録されている指紋データがリストとして、表示部６に表示され、削除したい指紋データを選択することができる。

【００９６】また、本件ではパスワードの削除を行なうと自動的にそれに対応した指紋も削除される。1人のユーザが複数の指を登録していた場合でも、そのユーザのすべての指紋データが削除される。このように、パスワードと関連付けて指紋データの登録／削除を行なうことで、指紋データのみに依存しないシステムとしている。これは、指紋データのみの認証では、指紋が傷ついた時などにシステムの起動ができなくなるためであり、本発明では、指紋認証はあくまでもパスワード認証の代替として機能するものである。

【００９７】上述したように、本発明によれば、指紋データ若しくはパスワードのどちらかによって、パソコンへのログイン認証を行なうことが可能となる。

【００９８】また、本実施形態では、生体データとして指紋データを用いた例を示したが、その他の生体データ認証として音声認証、顔認証、ハンドライティング署名認証等が考えられる。これらの場合、指紋センサ２の替りに、マイク、カメラ、ペン入力インターフェースが必要となるが、上述した実施例と同様の方法をＯＳ起動前に行なうことによりパスワードまたは生体データ（音声認証、顔認証、ハンドライティング署名など）のどちらか一方によるユーザ認証により、ＯＳを起動することができる。

【００９９】

【発明の効果】以上詳述した発明によれば、ＯＳ起動前のユーザ認証方法として、パスワードか生体データのどちらか一方が登録しておいたデータと一致すればＯＳが起動する電子機器の起動方法を提供することが可能である。

【図面の簡単な説明】

【図１】電子機器システムのハードウェア構成図。

【図２】電子機器システムの斜視図。

【図３】指紋認証プログラムのフローチャート。

【図４】ユーザ認証処理のフローチャート。

【図５】登録した指紋データが無い場合の表示画面例の図。

【図６】登録した指紋データはあるが、指紋センサが無い場合の表示画面例の図。

【図７】登録した指紋データと指紋センサとがある場合の表示画面例の図。

【図８】認証に成功した場合の表示画面例の図。

【図９】指紋認証初期表示画面例の図。

【図１０】指紋データが読み取れた場合の表示画面例の図。

【図１１】認証に失敗した場合の表示画面例の図。

【図１２】指紋認証処理を行なった場合の表示画面例の図。

【図１３】サスペンド、休止状態からの復帰フローチャート。

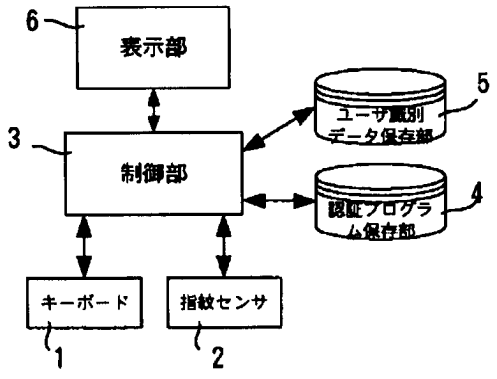
【図１４】指紋ユーティリティソフトの画面例の図。

【図１５】指紋データの登録フローチャート。

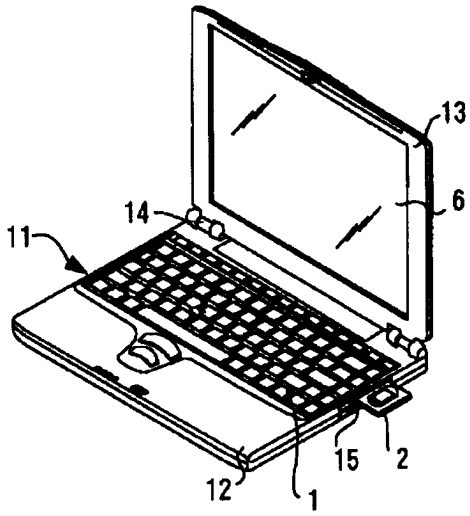
【符号の説明】

１…キーボード
２…指紋センサ
３…制御部
４…認証プログラム保存部
５…ユーザ識別データ保存部
６…表示部
１１…電子機器システム
１２…本体部ケース
１３…表示部ケース
１４…ヒンジ部

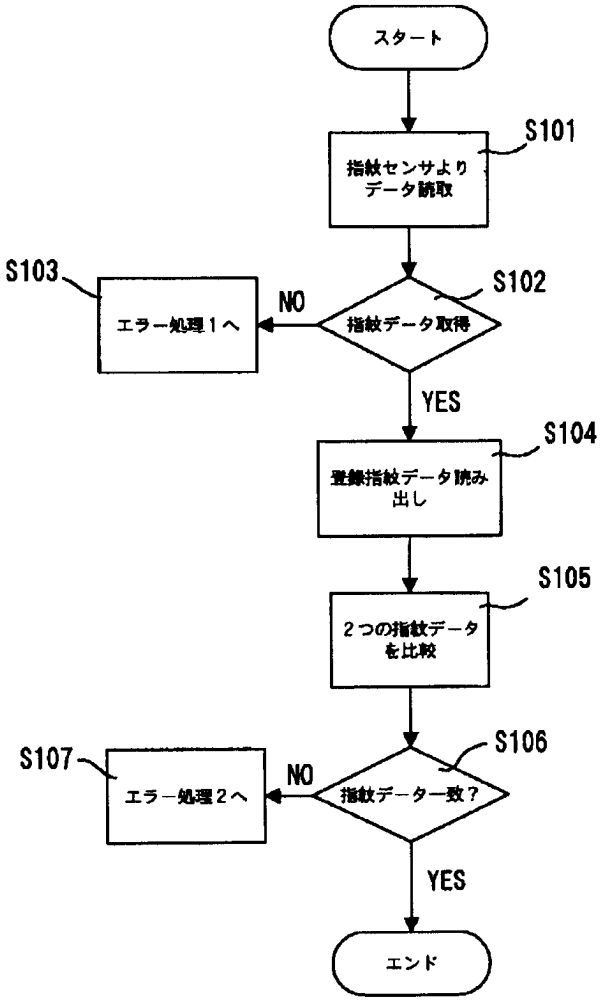
【図１】



【図２】

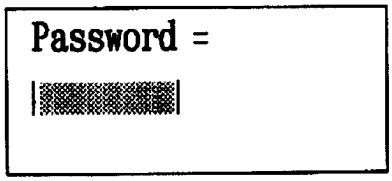


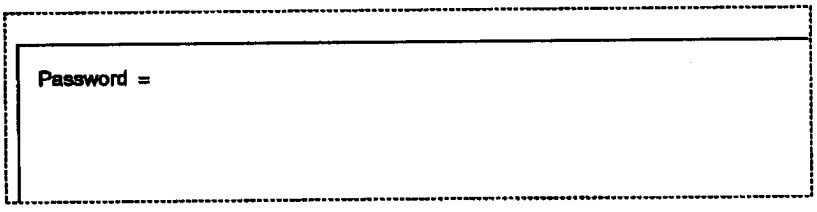
【図３】



【図５】

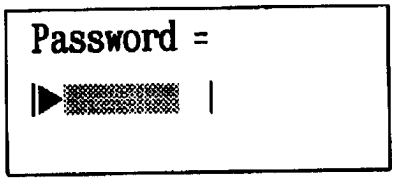
【図９】

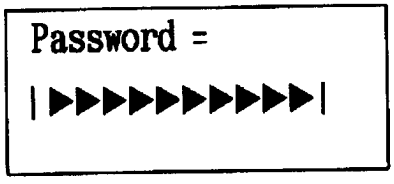




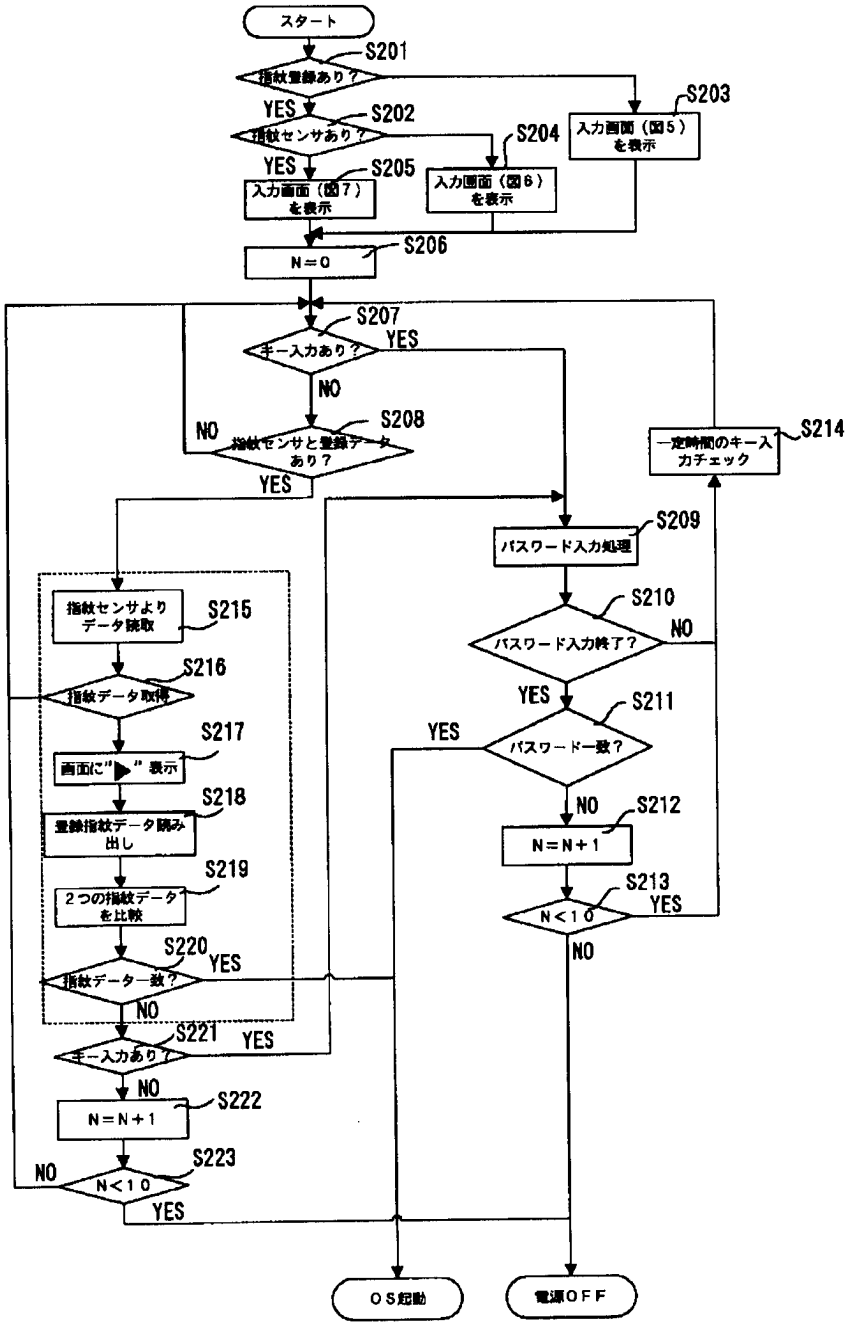
【図１０】

【図１２】

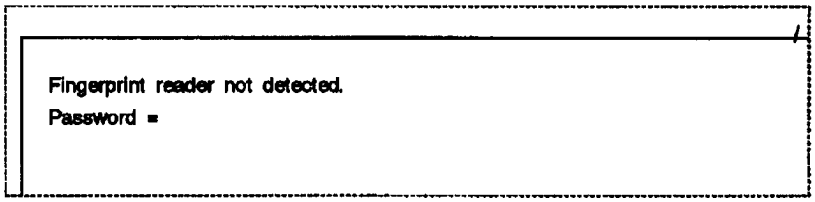




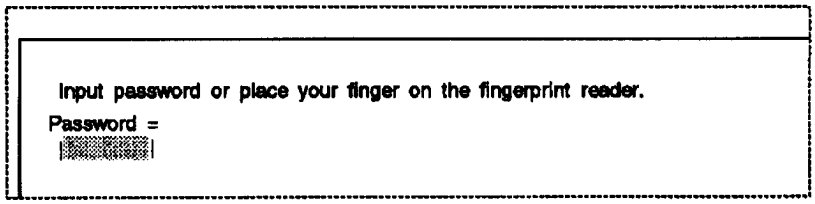
【図４】


スタート
S201
指紋登録あり？
YES
S202
指紋センサあり？
YES
S205
入力画面（図７）を表示
S203
入力画面（図５）を表示
S204
入力画面（図６）を表示
S206
N＝０
S207
キー入力あり？
YES
NO
S208
指紋センサと登録データあり？
NO
YES
S214
一定時間のキー入力チェック
S209
パスワード入力処理
S210
パスワード入力終了？
NO
YES
S211
パスワード一致？
YES
NO
S212
N＝N＋１
S213
N＜１０
YES
NO
S215
指紋センサよりデータ読取
S216
指紋データ取得
S217
画面に“▶”表示
S218
登録指紋データ読み出し
S219
２つの指紋データを比較
S220
指紋データ一致？
YES
NO
S221
キー入力あり？
YES
NO
S222
N＝N＋１
S223
N＜１０
NO
YES
OS起動
電源OFF

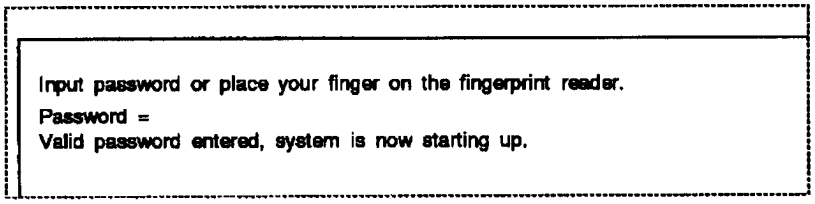
【図６】



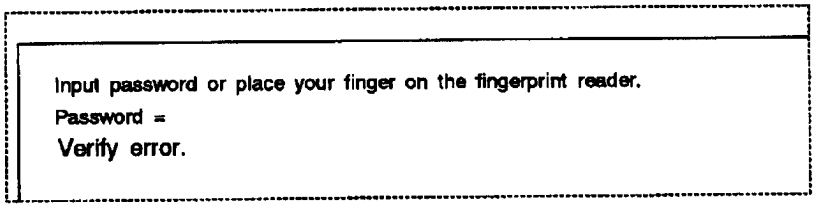
【図７】



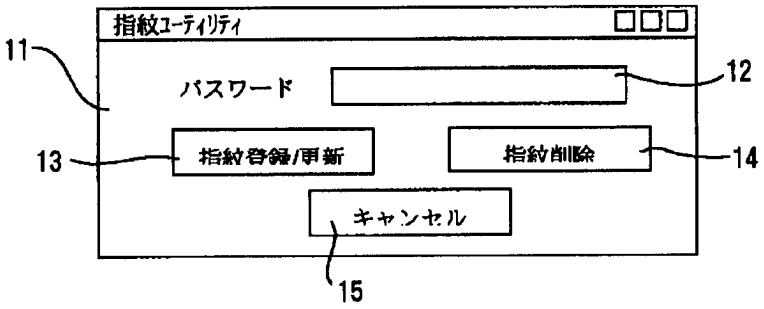
【図８】



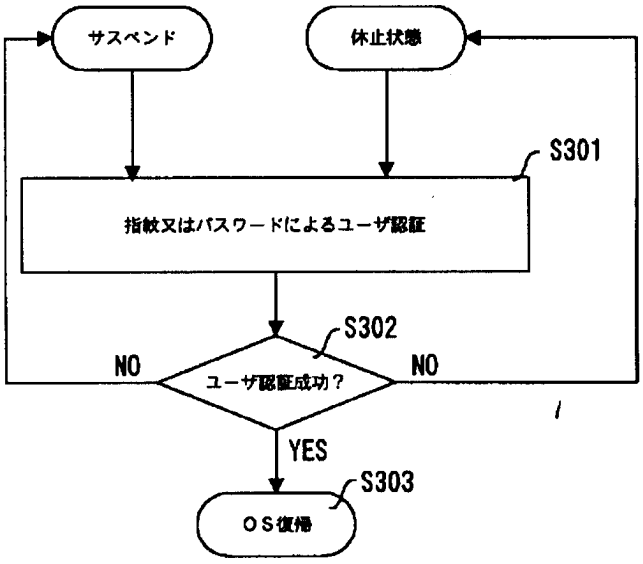
【図１１】



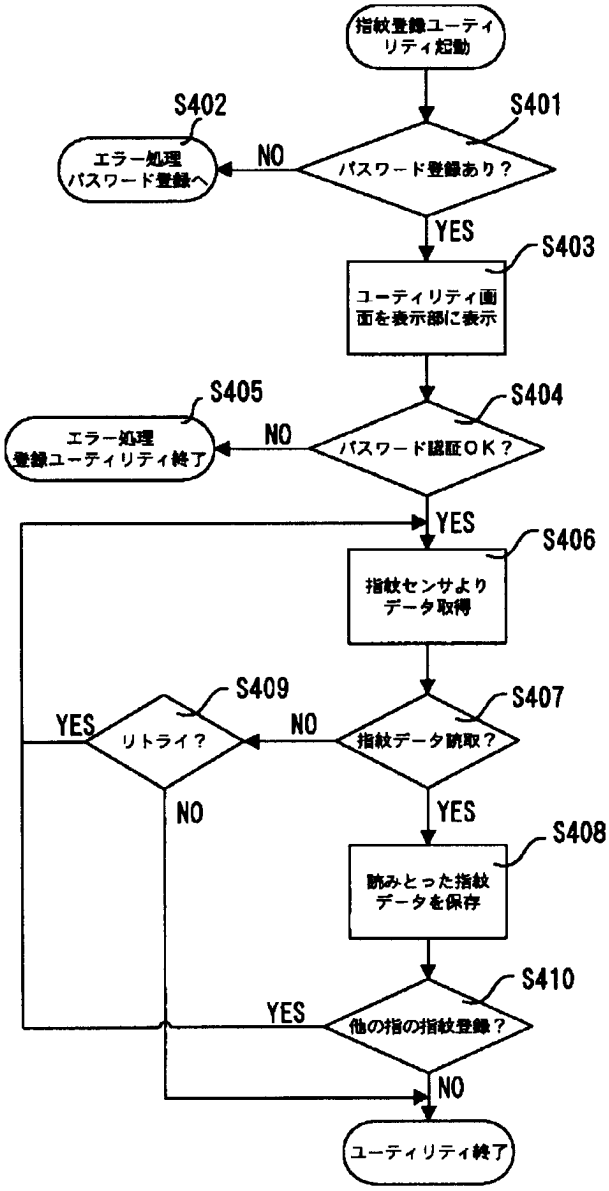
【図１４】



【図１３】


サスペンド
休止状態
S301
指紋又はパスワードによるユーザ認証
S302
NO
ユーザ認証成功？
NO
YES
S303
ＯＳ復帰

【図１５】


指紋登録ユーティリティ起動
S401
パスワード登録あり？
NO
S402
エラー処理
パスワード登録へ
YES
S403
ユーティリティ画面を表示部に表示
S404
パスワード認証ＯＫ？
NO
S405
エラー処理
登録ユーティリティ終了
YES
S406
指紋センサよりデータ取得
S407
指紋データ読取？
NO
S409
リトライ？
YES
NO
YES
S408
読みとった指紋データを保存
S410
他の指の指紋登録？
YES
NO
ユーティリティ終了